Journal of Number Theory 129 (2009) 3059–3068

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

p-Adic liftings of the supersingular j-invariants and j-zeros of certain Eisenstein series

P. Guerzhoy *,[1], Z. Kent

Department of Mathematics, University of Hawaii, 2565 McCarthy Mall, Honolulu, HI 96822-2273, United States

ARTICLE INFO

Article history:
Received 18 December 2008
Available online 14 August 2009
Communicated by David Goss

MSC:
11F11
11F33

ABSTRACT

Let $p > 3$ be a prime. We consider j-zeros of Eisenstein series E_k of weights $k = p - 1 + Mp^a(p^2 - 1)$ with $M, a \geqslant 0$ as elements of $\overline{\mathbb{Q}}_p$. If $M = 0$, the j-zeros of E_{p-1} belong to $\mathbb{Q}_p(\zeta_{p^2-1})$ by Hensel's lemma. Call these j-zeros p-adic liftings of supersingular j-invariants. We show that for every such lifting u there is a j-zero r of E_k such that $ord_p(r - u) > a$. Applications of this result are considered. The proof is based on the techniques of formal groups.

Published by Elsevier Inc.

1. Statement and discussion of results

Zeros of modular forms is an interesting subject, and there has been a big amount of research connected to this subject during the past several decades (see [1–3,5,14] to name a few). Zeros of Eisenstein series attract special attention. For an even integer $k \geqslant 4$ denote by E_k the weight k Eisenstein series

$$E_k = 1 - \frac{2k}{B_k} \sum_{n \geqslant 1} \left(\sum_{d|n} d^{k-1} \right) q^n, \qquad q = \exp(2\pi i \tau), \quad \Im\tau > 0,$$

where the B_k are Bernoulli numbers defined by the power series $x/(\exp(x) - 1) = \sum_{k \geqslant 0} B_k \frac{x^k}{k!}$. Following the terminology of [5], we define j-zeros to be the j-invariants of zeros of E_k. Denote by $\Psi_k(X)$ the polynomial that encodes the j-zeros of E_k:

$$\Psi_k(X) = \prod_{\substack{j = j(\tau), \\ \text{where } E_k(\tau) = 0}} (X - j).$$

* Corresponding author.
E-mail addresses: pavel@math.hawaii.edu (P. Guerzhoy), zach@math.hawaii.edu (Z. Kent).

[1] Supported by NSF grant DMS-0700933.

0022-314X/$ – see front matter Published by Elsevier Inc.
doi:10.1016/j.jnt.2009.06.006

Let $p > 3$ be a prime. The coefficients of Ψ_{p-1} are p-integral. It is a well-known observation of Deligne (see [9] for a full exposition) that $\widetilde{\Psi}_{p-1}(X)$, the modulo p reduction of $\Psi_{p-1}(X)$, is the supersingular polynomial at p. The roots of $\widetilde{\Psi}_{p-1}(X)$ over $\overline{\mathbb{F}}_p$ are supersingular j-invariants. This polynomial, considered as a polynomial over $\mathbb{F}_p$, splits into a product of factors over $\mathbb{F}_p$,

$$\widetilde{\Psi}_{p-1}(X) = \prod_i \widetilde{\psi}_i(X), \tag{1}$$

where the monic polynomials $\widetilde{\psi}_i(x) \in \mathbb{F}_p[X]$ are either linear or irreducible quadratic. In this paper we consider Ψ_k as a polynomial over the field of p-adic numbers $\mathbb{Q}_p$. A standard application of Hensel's lemma allows us to lift the supersingular j-invariants to characteristic zero in a canonical way. The possible presence of irreducible (over $\mathbb{F}_p$) quadratic factors in decomposition (1) makes it necessary to introduce the unique (see [12, Section 3.3]) unramified quadratic extension $K = \mathbb{Q}_p(\zeta)$ of $\mathbb{Q}_p$, where ζ is a primitive root of unity of degree $p^2 - 1$. The ring of integers of K will be denoted as $\mathcal{O}$. The following proposition is an immediate consequence of Hensel's lemma.

Proposition 1. *For every irreducible factor $\widetilde{\psi}_i(X)$ in decomposition (1) there are exactly $\deg(\widetilde{\psi}_i(X))$ elements $u \in \mathcal{O}$ such that*

$$\widetilde{\psi}_i(u) \equiv 0 \mod p \quad \text{and} \quad \Psi_{p-1}(u) = 0.$$

This proposition motivates the following definition.

Definition 1. We call an element $u \in \mathcal{O}$ from Proposition 1 a lifting of a supersingular j-invariant to characteristic zero.

Throughout the paper

$$k = k(a, M) = p - 1 + Mp^a\left(p^2 - 1\right)$$

with non-negative integers a and M. The subject of investigation in this paper is the polynomial $\Psi_k(X)$ and its zeros.

Define $\epsilon = \epsilon(p), \gamma = \gamma(p) \in \{0, 1\}$ such that

$$\epsilon \equiv \frac{p-1}{4} \mod 3 \qquad \text{and} \quad \gamma \equiv \frac{p-1}{6} \mod 2.$$

Let $\delta(k) = \lfloor k/12 \rfloor$. We define the polynomial $\varphi_k(X)$ (found in [5]) by:

$$\Psi_k(X) = X^\epsilon (X - 1728)^\gamma \varphi_k(X). \tag{2}$$

A result of Gekeler [5, Corollary 2.6] implies the following factorization over $\mathbb{F}_p$

$$\widetilde{\varphi}_k(X) = \widetilde{\varphi}_{p-1}(X)^{d+1} X^{\epsilon d/3} (X - 1728)^{\gamma d/2} \tag{3}$$

where $d = M(p^{a+1} + p^a)$. Note that all exponents in this factorization are integers. This factorization implies, in particular, that

$$\Psi_k(u) \equiv 0 \mod p$$

for every lifting u of a supersingular j-invariant, and it is natural to ask about a connection between the roots of the polynomials $\Psi_{p-1}(X)$ and $\Psi_k(X)$. Numerical examples show that the roots of $\Psi_k(X)$

may not belong to K. We thus consider these roots as elements of the algebraic closure $\overline{\mathbb{Q}}_p$ of $\mathbb{Q}_p$. Our principal result provides a partial answer to the above question.

Theorem 1. *Let u be a lifting of a supersingular j-invariant. There is $r \in \overline{\mathbb{Q}}_p$ such that $\Psi_k(r) = 0$ and*

$$ord_p(r-u) > a.$$

If $p > 13$, the polynomial $\Psi_k(X)$ is not irreducible. Indeed, since the Galois group preserves distances (cf. e.g. [12, Chapter 3]), the factorizations (1), (2), and (3) imply the following factorization over $\mathbb{Q}_p$:

$$\Psi_k(X) = \prod_u \psi_{u,k}(X). \tag{4}$$

The product in (4) is taken over all pairwise non-conjugate by $Gal(K/\mathbb{Q}_p)$ liftings u of supersingular j-invariants. The polynomials $\psi_{u,k}(X) \in \mathbb{Z}_p[x]$ are monic of degree

$$\deg \psi_{u,k}(X) = \big(d/e(u) + 1\big) \deg \widetilde{\psi}_u = \big(M\big(p^{a+1} + p^a\big)/e(u) + 1\big) \deg \widetilde{\psi}_u,$$

where $e(u)$ is the ramification degree of the relevant j-zero, i.e.

$$e(u) = \begin{cases} 3 & \text{if } u \equiv 0 \bmod p, \\ 2 & \text{if } u \equiv 1728 \bmod p, \\ 1 & \text{otherwise.} \end{cases}$$

In particular, when $M = 0$, and $k(a,0) = p-1$, we drop the index k by setting

$$\psi_u = \psi_{u,p-1}.$$

There are speculations, based on numerical evidence, on the irreducibility of the polynomials Ψ_k over $\mathbb{Q}$. The above remarks show that over $\mathbb{Q}_p$ a similar question is meaningful only about the individual polynomials $\psi_{u,k}$. As an application to Theorem 1, we prove the reducibility of every factor $\psi_{u,k}$ of Ψ_k over $\mathbb{Q}_p$.

Theorem 2. *If $M \geqslant 1$ and $a \geqslant 1$, then $\psi_{u,k}(X)$ is reducible over $\mathbb{Q}_p$ for every u.*

In contrast, our next result implies, in particular, that the polynomials $\psi_{u,k}$ typically do not split completely over K.

Theorem 3. *If $M \geqslant 1$, then the splitting field of the polynomial $\psi_{u,k}$ is ramified over $\mathbb{Q}_p$ for every u such that $e(u) \leqslant a$.*

In Section 2 of the paper we state certain congruences between special values of the polynomials ψ_u and $\psi_{u,k}$ (Theorem 4), and derive our results from these congruences. Section 3 is devoted to the proof of Theorem 4. This proof involves the techniques of formal groups. In particular, Proposition 4 claims congruences for the coefficients of series expansions of certain functions on Lubin–Tate formal groups of height 2. The proof of this proposition, which is an adaptation to our setting of an argument invented by Katz [11] (see also [4] for a refinement) is deferred to Section 4.

2. Proofs of the main results

We preserve the notations introduced in Section 1, in particular, $u \in K$ is a lifting of a supersingular j-invariant. In this section, we derive our main results from the following congruences:

Theorem 4. *Let $s \in K$ be such that $ord_p(\psi_u(s)) \in e(u)\mathbb{Z}$.*

(a) *If $0 < ord_p(\psi_u(s)) < a+1$, then*

$$ord_p\big(\psi_{u,k}(s)\big) = Mp^{a+1} + ord_p\big(\psi_u(s)\big).$$

(b) *If $ord_p(\psi_u(s)) \geqslant a+1$, then*

$$ord_p\big(\psi_{u,k}(s)\big) \geqslant Mp^{a+1} + a + 1.$$

Proof of Theorem 1. If $e(u) > 1$, the statement is trivial in view of (2) and (3). We thus assume that $e(u) = 1$.

We denote by $r_l \in \overline{\mathbb{Q}}_p$ the roots of the polynomial $\psi_{u,k}(X)$:

$$\psi_{u,k}(X) = \prod_l (X - r_l).$$

Choose $s_1, s_2 \in \mathcal{O}$ such that $ord_p(s_1 - u) = a$ and $ord_p(s_2 - u) \geqslant a+1$. Since K is unramified, we have

$$ord_p\big(\psi_u(s_1)\big) = a \quad \text{and} \quad ord_p\big(\psi_u(s_2)\big) \geqslant a+1.$$

If $ord_p(r_l - u) \leqslant a$, then the ultrametric inequality implies that

$$ord_p(s_2 - r_l) = ord_p(r_l - u) \leqslant ord_p(s_1 - r_l).$$

We now assume that $ord_p(r_l - u) \leqslant a$ for all roots r_l, and make use of Theorem 4 to obtain a contradiction:

$$a + 1 + Mp^{a+1} \leqslant ord_p\big(\psi_{u,k}(s_2)\big) \leqslant ord_p\big(\psi_{u,k}(s_1)\big) = a + Mp^{a+1}.$$

Theorem 1 follows from this observation. □

Proof of Theorem 2. As in the proof of Theorem 1, we assume that $e(u) = 1$, because otherwise the result is immediate from (2) and (3).

Choose $s \in K$ such that $ord_p(\psi_u(s)) = 1$. By Theorem 1 there is a root r_0 of $\psi_{u,k}$ and $ord_p(r_0 - u) > a \geqslant 1$. Therefore $ord_p(s - r_0) = 1$. If we assume that $\psi_{u,k}$ is irreducible, then because the Galois group preserves distances and all roots are conjugate, we must have $ord_p(s - r_l) = ord_p(s - r_0)$ for all roots r_l. But this leads to a contradiction of Theorem 4,

$$ord_p\big(\psi_{u,k}(s)\big) = \sum_l ord_p(s - r_l) = M\big(p^{a+1} + p^a\big) + 1 > Mp^{a+1} + 1,$$

proving our result. □

Proof of Theorem 3. Let $s_0 \in K$ be such that $s_0 \equiv u \bmod p^{e(u)}$ and s_0 is not congruent modulo $p^{e(u)+1}$ to a lifting of a supersingular j-invariant. By Theorem 4

$$ord_p\big(\psi_{u,k}(s_0)\big) = Mp^{a+1} + e(u).$$

On the other hand, if we assume that the splitting field of $\psi_{u,k}$ is unramified, then $ord_p(s_0 - r_l) \geqslant e(u)$, and we have the contradiction

$$\begin{aligned} ord_p\big(\psi_{u,k}(s_0)\big) &= \sum_l ord_p(s_0 - r_l) \\ &\geqslant e(u)\big(M\big(p^{a+1} + p^a\big)/e(u) + 1\big) \\ &> Mp^{a+1} + e(u). \qquad \square \end{aligned}$$

3. Proof of Theorem 4

In this section we prove Theorem 4 with the help of several propositions; one whose proof is postponed to the next section. We derive Theorem 4 from a certain congruence (see Proposition 2 below) for Bernoulli–Hurwitz numbers [10,11]. The authors know two parallel ways to prove this congruence. Firstly, since the formal group of the elliptic curve with j-invariant s has height 2 (the elliptic curve has supersingular reduction at p), one can make use of a corollary to Katz' general theorem on formal groups and p-adic interpolation [10, Corollary 3]. However, to the best of the authors' knowledge, the full proof of this theorem has never been published. An alternative approach, which we undertake here, is based on a later observation of Katz [11] (see also [4] for refinements). Namely, one proves that the formal group in question is isomorphic to a Lubin–Tate formal group, and applies an elementary argument which implies the desired congruences.

We preserve the notations of the previous sections.

Proposition 2. *Let $s \in K$ be such that $0 < ord_p(\Psi_{p-1}(s)) \in e(u)\mathbb{Z}$ for some lifting u of a supersingular j-invariant. Let $b \in \mathbb{Z}$ be an integer different from 1 and coprime to p. Define*

$$T(l) = \frac{(1-b^l)(1-p^{l-2})}{p^{\lfloor (l-2)p/(p^2-1)\rfloor}} \frac{B_l}{l} \Psi_l(s).$$

Then for some $\mu \in \mathcal{O}$ such that $ord_p(\mu) = 0$ we have the congruences

$$\mu T(p-1) \equiv T(k) \mod p^{a+1}.$$

Proof of Theorem 4. Let l be a positive integer that is a multiple of $p-1$. (Note that $(p-1) \mid k$.) By von Staudt congruences, $ord_p(B_l) = -1$. Fermat's Little Theorem and the Binomial Theorem imply that $ord_p(1-b^l) = 1 + ord_p(l)$. In order to derive Theorem 4 from Proposition 2, we simply equate the p-orders of the congruences of Proposition 2 and use the factorization (4). $\square$

The proof of Proposition 2 is more involved, and requires some preliminaries on one-dimensional formal groups. For a formal group F we denote by $[p]_F \in End(F)$ the multiplication by p map. If $\alpha \in \mathcal{O}$ is a unit, then the Lubin–Tate lemma [13] implies the existence and uniqueness up to isomorphism of a height two one-parameter formal group $G(\alpha)$ over $\mathcal{O}$ such that

$$[p]_{G(\alpha)}(X) = pX + \alpha X^{p^2}.$$

Proposition 3. *Let F be the formal group over $\mathcal{O}$ of the elliptic curve E defined by the equation*

$$y^2 = 4x^3 - g_2x - g_3, \quad g_2, g_3 \in \mathcal{O}, \tag{5}$$

with j-invariant

$$s = \frac{1728g_2^3}{g_2^3 - 27g_3^2}.$$

If $\Psi_{p-1}(s) \equiv 0 \bmod p$, then the discriminant $\Delta = g_2^3 - 27g_3^2$ is a unit, $ord_p(\Delta) = 0$, and F is isomorphic to a formal group $G(\alpha)$ with

$$[p]_{G(\alpha)}(X) = pX + \alpha X^{p^2}.$$

Proof. A well-known observation of Deligne (see e.g. [9, p. 105] for a proof) is that the modulo p reduction of the elliptic curve $\widetilde{E}$ (5) is a supersingular elliptic curve over $\mathcal{O}/(p)$. In particular, $ord_p(\Delta) = 0$. It follows (see [8, Table, p. 269], [15, Theorem IV.7.4]) that the p^2-power Frobenius endomorphism of $\widetilde{E}$ factors through the multiplication by p isogeny, $Frob = [p]\alpha^{-1}$, with a separable isogeny α. The latter is a multiplication by (a modulo p reduction of) $\alpha \in \mathcal{O}$ with $ord_p(\alpha) = 0$. This induces the factorization of the Frobenius endomorphism of the formal group $\widetilde{F}$ of $\widetilde{E}$, which is the modulo p reduction of F. We thus have

$$\left[p\alpha^{-1}\right]_F(X) \equiv X^{p^2} \mod p \quad \text{and} \quad [p\alpha^{-1}]_F(X) \equiv p\alpha^{-1}X \mod \deg 2,$$

where the second congruence holds in any formal group. An application of the Lubin–Tate lemma [13] establishes an isomorphism between F and a formal group G' over $\mathcal{O}$ with

$$[p]_{G'}(X) = p\alpha^{-1}X + X^{p^2}.$$

In order to finish the proof we note that both G' and $G(\alpha)$ have characteristic polynomial $t^2 - p\alpha^{-1}$ and are therefore isomorphic (see [6,7]). □

If a formal group F is defined over $\mathcal{O}$, then we call a formal power series $f \in \mathcal{O}[\![X]\!]$ a function on F. The invariant differentiation D acts on functions on F.

Proposition 4. *Let f be a function on $G(\alpha)$. Assume that f satisfies the difference equation*

$$\sum_{[p](\lambda)=0} f(X \underset{G(\alpha)}{+} \lambda) = 0. \tag{6}$$

Let

$$L_f(n) = \frac{D^n(f)(0)}{p^{\lfloor np/(p^2-1)\rfloor}}.$$

For all integers $n, a \geqslant 0$ with $n \not\equiv 0, p, 2p, \ldots, (p-1)p \bmod (p^2-1)$, the following congruence holds:

$$\left(\alpha\left(p^2-2\right)!p^{1-p}\right)^{p^a} L_f(n) \equiv L_f\left(n + p^a\left(p^2-1\right)\right) \mod p^{a+1}.$$

We postpone the proof of Proposition 4 to the next section.

In order to obtain Proposition 2 we consider the Laurent series expansion of the Weierstrass $\wp$-function associated with the elliptic curve E defined by (5)

$$\wp(E,z) = z^{-2} - \sum_{m\geqslant 1} \frac{B_{2m+2}}{2m+2}(2\pi i)^{2m+2} E_{2m+2} \frac{z^{2m}}{(2m)!}. \tag{7}$$

Note that $\wp(E,z) \in K[\![z^{-1}, z]\!]$ since $(2\pi i)^l E_l$ is a polynomial in g_2 and g_3 with rational coefficients for even $l \geqslant 4$.

The parameter of the formal group corresponding to the elliptic curve E is $X = -2\wp(E,z)/\wp'(E,z)$, and the power series expansion of $\wp$ in X belongs to $\mathcal{O}[\![X^{-1}, X]\!]$ (see [15, Chapter IV, §1]). The series $\wp$ is not a function on this formal group only due to the pole at zero. This deficiency is, however, easily fixed. For an integer $N \in \mathbb{Z}$ and a power series $g \in \mathcal{O}[\![X^{-1}, X]\!]$, put as in [4,11]

$$[N]^* g(X) = g\big([N]X\big).$$

Note that in terms of the parameter z we simply have $[N]^*\wp(E,z) = \wp(E, Nz)$.

Proposition 5. *Let $b \in \mathbb{Z}$ be an integer different from 1 and coprime to p. The power series in X*

$$\wp_{b,p}(E,X) = \big(1 - [p]^*\big)\big(1 - b^2[b]^*\big)\wp(E,X)$$

is a function on the formal group of an elliptic curve E, and satisfies the difference equation (6)*.*

Proof. We adopt the desired identity to the logarithmic parameter z, which we consider as the usual complex variable. Let Λ be the period lattice of the elliptic curve E. The claimed identity becomes

$$\sum_{\lambda} \big(1 - [p]^*\big)\big(1 - b^2[b]^*\big)\wp(E, z+\lambda) = 0,$$

where the summation is taken over all points λ in the fundamental parallelogram of Λ such that $p\lambda \in \Lambda$. In order to check the latter identity it suffices to notice that the function on the left-hand side is Λ-periodic, equals zero at the points of Λ, and has no poles in the fundamental parallelogram of Λ. □

Proof of Proposition 2. By hypothesis and the factorization (3), we have $s \in \mathcal{O}$ such that $0 < ord_p(s-u) \in e(u)\mathbb{Z}$. This allows us to choose $g_2, g_3 \in \mathcal{O}$ such that s is the j-invariant of the elliptic curve (5) as follows:

If $s \equiv 0 \bmod p$, then $u = 0$ and $ord_p(s) \in 3\mathbb{Z}$, so we may write $s = \nu p^{3k}$ for some unit $\nu \in \mathcal{O}$ and positive integer k. Consider the equation

$$s = 1728\frac{g_2^3}{g_2^3 - 27g_3^2} = 1728\frac{(g_2/3)^3}{(g_2/3)^3 - g_3^2},$$

with variables g_2 and g_3. Taking $g_2 = -\frac{p^k}{4\nu} \in \mathcal{O}$ in the equation, we may rewrite the result as a polynomial equation over $\mathbb{Z}_p$ with variable g_3:

$$g_3^2 + \frac{p^{3k}}{1728\nu^3} - \frac{1}{\nu^4} = 0.$$

This polynomial has a pair of simple nonzero roots when considered modulo p. Therefore a standard application of Hensel's lemma allows us to find a solution $g_3 \in \mathcal{O}$. For all other choices of s, we may choose $g_2, g_3 \in \mathcal{O}$ in a similar way.

Combining Propositions 5, 3, and 4 we obtain the congruences

$$\left(\alpha\left(p^2-2\right)!p^{1-p}\right)^{Mp^a} L_{\wp_{b,p}}(n) \equiv L_{\wp_{b,p}}\left(n+Mp^a\left(p^2-1\right)\right) \mod p^{a+1} \tag{8}$$

where $n \not\equiv 0, p, 2p, \ldots, (p-1)p \bmod (p^2-1)$ and $\alpha(p^2-2)!p^{1-p}$ is a unit in $\mathcal{O}$. We need only consider the case when $n = p-3$.

For all positive even integers l,

$$D^l(\wp_{b,p})(0) = -\left(1-b^{l+2}\right)\left(1-p^l\right)\frac{B_{l+2}}{l+2}(2\pi i)^{l+2}E_{l+2}.$$

By [5, Proposition 1.17],

$$(2\pi i)^k E_k = \varphi_k(s)\Delta^{\delta(k)}(12g_2)^{\epsilon}(-216g_3)^{\gamma}.$$

Combining the above equalities with (2), we find that

$$T(k) = -L_{\wp_{b,p}}(k-2)\left(\frac{144g_2^2}{\Delta}\right)^{\epsilon}\left(\frac{-216g_3}{\Delta}\right)^{\gamma}\Delta^{-\delta(k)}.$$

Therefore, upon multiplying the congruences (8) by the integral factor

$$-\left(\frac{144g_2^2}{\Delta}\right)^{\epsilon}\left(\frac{-216g_3}{\Delta}\right)^{\gamma}\Delta^{-\delta(k)}$$

(Δ is a unit in $\mathcal{O}$ by Proposition 3), and taking

$$\mu := \Delta^{\delta(p-1)-\delta(k)}\left(\alpha\left(p^2-2\right)!p^{1-p}\right)^{Mp^a},$$

we obtain the congruences of Proposition 2. □

4. Proof of Proposition 4

In this section we prove Proposition 4 closely following [4,11]. Recall that $p > 3$ (this restriction slightly simplifies the argument).

Let $\mathcal{O}$ be a commutative ring with identity and G a one parameter (commutative) formal group over $\mathcal{O}$ with parameter X and group law $F(X,Y) = X +_G Y \in \mathcal{O}[\![X,Y]\!]$. We will identify the coordinate ring of G with $\mathcal{O}[\![X]\!]$. As in [11] we denote by $\mathrm{Diff}(G)$ the commutative $\mathcal{O}$-algebra of all G-invariant $\mathcal{O}$-linear differential operators of $\mathcal{O}[\![X]\!]$. As an $\mathcal{O}$-module, $\mathrm{Diff}(G)$ is free with basis $D(n), n = 0, 1, 2, \ldots$ defined by "Taylor expansion" for all $f \in \mathcal{O}[\![X]\!]$ by

$$f(X \underset{G}{+} Y) = \sum_{n \geqslant 0} D(n)(f)Y^n \in \mathcal{O}[\![X,Y]\!].$$

The operator $D(0)$ is the identity in $\mathcal{O}[\![X]\!]$, and $D(1)$ is the G-invariant derivation, normalized by $D(X)(0) = 1$, which we will denote by D. Recall that (see [11, Identity 2.4]) for $0 \leqslant n \leqslant p^2-1$

$$D(n) = \frac{D^n}{n!}. \tag{9}$$

Let $\widehat{\mathrm{Diff}}(G(\alpha))$ be the p-adic completion of $\mathrm{Diff}(G(\alpha))$, then we can define an operator

$$H = \frac{p^2-1}{p^2}\sum_{r\geqslant 2}(-p/\alpha)^r D\big(r\big(p^2-1\big)\big) \in \widehat{\mathrm{Diff}}\big(G(\alpha)\big),$$

For convenience of notation, we also define the operator (as in [4])

$$X_o = 1 + H \in \widehat{\mathrm{Diff}}\big(G(\alpha)\big).$$

We need the following congruences proved in [4, pp. 168–169]

$$DH \equiv 0 \mod p\widehat{\mathrm{Diff}}\big(G(\alpha)\big), \tag{10}$$

and for a non-negative integer n

$$D^n \equiv 0 \mod p^{\lfloor np/(p^2-1)\rfloor}\widehat{\mathrm{Diff}}\big(G(\alpha)\big), \tag{11}$$

$$H^n \equiv 0 \mod p^{\lfloor n(1-1/p)\rfloor}\widehat{\mathrm{Diff}}\big(G(\alpha)\big). \tag{12}$$

We must show that

$$L_f\big(n+p^a\big(p^2-1\big)\big) \equiv \big(\alpha\big(p^2-2\big)!p^{1-p}\big)^{p^a} L_f(n) \mod p^{a+1}$$

for $n \not\equiv 0, p, 2p, \ldots, (p-1)p \bmod (p^2-1)$. The difference equation (6) and the identity (9) imply

$$X_o = \frac{p^2-1}{\alpha p} D\big(p^2-1\big) = \frac{D^{p^2-1}}{\alpha p(p^2-2)!}.$$

It follows that

$$\left(\frac{p^{p-1}}{\alpha(p^2-2)!}\right)^{p^a} L_f\big(n+p^a\big(p^2-1\big)\big) - L_f(n) = \big(X_o^{p^a}-1\big)L_f(n) = D\big(X_o^{p^a}-1\big)\frac{D^{n-1}}{p^{\lfloor np/(p^2-1)\rfloor}}(f)(0).$$

Since $\lfloor (n-1)p/(p^2-1)\rfloor = \lfloor np/(p^2-1)\rfloor$ for $n \not\equiv 0, p, 2p, \ldots, (p-1)p \bmod (p^2-1)$, (see [11, §3]), the congruence (11) implies that $D^{n-1} \equiv 0 \mod p^{\lfloor np/(p^2-1)\rfloor}\widehat{\mathrm{Diff}}(G(\alpha))$. It thus suffices to show that $D(X_0^{p^a}-1) \equiv 0 \mod p^{a+1}\widehat{\mathrm{Diff}}(G(\alpha))$. For $a=0$, this coincides with (10). For $a \geqslant 1$,

$$\begin{aligned} D\big(X_0^{p^a}-1\big) &= D(1+H)^{p^a} - D \\ &= p^a DH + \sum_{k=2}^{p^a}\binom{p^a}{k} DH^k \\ &\equiv 0 \mod p^{a+1}\widehat{\mathrm{Diff}}\big(G(\alpha)\big). \end{aligned}$$

The latter congruence follows from (10), the obvious inequality $\lfloor (k-1)(1-1/p)\rfloor \geqslant ord_p(k)$ for $k \geqslant 2$, and the following calculation:

$$\begin{aligned}\binom{p^a}{k} DH^k &= \binom{p^a-1}{k-1}\frac{p^a}{k}(DH)H^{k-1}\\ &\equiv 0 \mod p^{a-ord_p(k)+1+\lfloor (k-1)(1-1/p)\rfloor}\widehat{\mathrm{Diff}}\big(G(\alpha)\big)\end{aligned}$$

by (10) and (12).

References

[1] Scott Ahlgren, Ken Ono, Weierstrass points on $X_0(p)$ and supersingular j-invariants, Math. Ann. 325 (2) (2003) 355–368.
[2] Tetsuya Asai, Masanobu Kaneko, Hirohito Ninomiya, Zeros of certain modular functions and an application, Comment. Math. Univ. St. Pauli 46 (1) (1997) 93–101.
[3] Jan H. Bruinier, Winfried Kohnen, Ken Ono, The arithmetic of the values of modular functions and the divisors of modular forms, Compos. Math. 140 (3) (2004) 552–566.
[4] Mustapha Chellali, Congruences entre nombres de Bernoulli–Hurwitz dans le cas supersingulier, J. Number Theory 35 (2) (1990) 157–179.
[5] Ernst-Ulrich Gekeler, Some observations on the arithmetic of Eisenstein series for the modular group $\mathrm{SL}(2,\mathbb{Z})$. Festschrift: Erich Lamprecht, Arch. Math. (Basel) 77 (1) (2001) 5–21.
[6] Walter L. Hill, Formal groups and zeta-functions of elliptic curves, Invent. Math. 12 (1971) 321–336.
[7] Taira Honda, On the theory of commutative formal groups, J. Math. Soc. Japan 22 (1970) 213–246.
[8] Dale Husemöller, Elliptic Curves, second ed., with appendices by Otto Forster, Ruth Lawrence and Stefan Theisen in: Grad. Texts in Math., vol. 111, Springer-Verlag, New York, ISBN 0-387-95490-2, 2004, xxii+487 pp.
[9] M. Kaneko, D. Zagier, Supersingular j-invariants, hypergeometric series, and Atkin's orthogonal polynomials, in: Computational Perspectives on Number Theory, Chicago, IL, 1995, in: AMS/IP Stud. Adv. Math., vol. 7, Amer. Math. Soc., Providence, RI, 1998, pp. 97–126.
[10] Nicholas M. Katz, Formal groups and p-adic interpolation, in: Journées Arithmétiques de Caen, Univ. Caen, Caen, 1976, Asterisque 41–42 (1977) 55–65, Soc. Math. France, Paris.
[11] Nicholas M. Katz, Divisibilities, congruences, and Cartier duality, J. Fac. Sci. Univ. Tokyo Sect. IA Math. 28 (3) (1981) 667–678, (1982).
[12] Neal Koblitz, p-Adic Numbers, p-Adic Analysis, and Zeta-Functions, second ed., Grad. Texts in Math., vol. 58, Springer-Verlag, New York, 1984.
[13] Jonathan Lubin, John Tate, Formal complex multiplication in local fields, Ann. of Math. (2) 81 (1965) 380–387.
[14] F.K.C. Rankin, H.P.F. Swinnerton-Dyer, On the zeros of Eisenstein series, Bull. London Math. Soc. 2 (1970) 169–170.
[15] Joseph H. Silverman, The Arithmetic of Elliptic Curves, corrected reprint of the 1986 original, Grad. Texts in Math., vol. 106, Springer-Verlag, New York, 1992.